REMARKS

These remarks are set forth in response to the Third Office Action. As this amendment has been timely filed within the three-month statutory period, neither an extension of time nor a fee is required. At the time of the Third Office Action, Claims 1 through 7 were pending and rejected in this application. Previously, Applicants cancelled claims 8 through 21 to remove these claims from further consideration in this application. Applicants are not conceding in this application that those claims are not patentable over the art cited by the Examiner, as the previous claim cancellations were only for facilitating expeditious prosecution of the present application. Applicants respectfully reserved the right to pursue these and other claims in one or more continuations and/or divisional patent applications.

CLAIMS 1-7 ARE REJECTED UNDER 35 U.S.C. § 103 FOR OBVIOUSNESS BASED UPON NGUYEN ET AL., U.S. APPLICATION PUBLICATION NO. 2004/0193865 (HEREINAFTER NGUYEN) IN VIEW OF NEVIS ET AL, U.S. PATENT NO. 6,581,159 (HEREINAFTER NEVIS)

On pages 2-3 of the Second Office Action, the Examiner asserted that one having ordinary skill in the art would have been realistically impelled to modify Nguyen in view of Nevis to arrive at the claimed invention. This rejection is respectfully traversed.

Claim 1

Independent claim 1 recites a method for "**reducing the boot time** of a Trusted Computing Performance Alliance (TCPA) based computing system" includes "executing a **boot block code** comprising a **Core Root of Trust for Measurement (CRTM)**". As an initial matter, there is no discussion or mention in Nguyen of "**reducing the boot time of a Trusted Computing Performance Alliance (TCPA) based computing system**" by "executing a **boot**

block code comprising a Core Root of Trust for Measurement (CRTM)". To the contrary, the Nguyen invention is specifically directed to a method for securely updating a basic input/output system (BIOS) using a multi-layer scheme." (see lines 1-2 of Abstract of Nguyen, emphasis added). Moreover, Nguyen explicitly states, "the new BIOS image is sent to the computer system in a BIOS capsule that also contains the data structure and instructions of how to build a new BIOS image for the computer system." (see lines -2 of Abstract of Nguyen, emphasis added). Thus, paragraph [0017] does not support the Examiner's conclusion that Nguyen discloses a method for "**reducing the boot time** of a ... **TCPA based** computing system".

Independent claim 1 further recites "**reading bits in a register** ... wherein **said bits in said register indicate whether segments of said flash memory have been updated**". On page 2 of the Third Office Action, the Examiner cited paragraph [0022] of Nguyen to teach " reading bits in register storing boot code, where register indicates whether segments have been updated." Applicants, however, disagree that this passage teaches the limitations for which Nguyen is being relied upon to teach. In contrast, paragraph [0022] of Nguyen teaches a "BIOS update process begins in a block 302, in which computer system 200 receives a new BIOS capsule 404." Thereafter, Nguyen teaches that two "checks" are made at decision block 306, a "correct capsule?" decision is checked, and at decision block 309, an "Admin Check Fail" decision is checked. If both checks are passed, then a new BIOS image from the new BIOS capsule can be performed, to proceed with a replacement of original BIOS image. (see FIG. 3 and lines 1-6 of paragraph [0023] of Nguyen. More importantly, there is no discussion in Nguyen of "**reading bits in a register** ... wherein **said bits in said register indicate whether segments of said flash**

memory have been updated". Thus, paragraph [0022] of Nguyen fails to teach the limitations for which the Examiner is relying upon Nguyen to teach.

To teach the claimed "**obtaining one or more measurement values** from a **table storing hashed values** from a **previous measurement** of a Power On Self Test (POST) Basic Input/Output System (BIOS) **if one or more of said bits in said register indicate one or more segments** of said flash memory storing said POST BIOS have not been updated" the Examiner cited Column 5, lines 15-25 of Nevis. However, upon reviewing the Examiner's cited passages Applicants are unable to identify where Nevis teaches "**obtaining one or more measurement values** from a **table storing hashed values** from a **previous measurement** of a POST BIOS **if one or more of said bits in said register indicate one or more segments** of said flash memory storing said POST BIOS have not been updated". Instead, Nevis merely teaches applying a one-way hash to the **external BIOS module** to obtain a computed hash value." (see Column 5, lines 12-15 of Nevis). Thus Nevis fails to teach the limitations for which the Examiner is relying upon Nevis to teach.

Regarding the Examiner's obviousness analysis, the Examiner asserted the following on page 4 of the First Office Action:

> It would be obvious to one having ordinary skill in the art at the time of the invention to include the hash values in the invention of Nguyen in order to verify/unlock the hardware as taught in Nevis see Col 5, Ln 21-24.

Applicants are unclear as to how the Examiner's proposed rationale for the combination would have led one having ordinary skill in the art to modify Nguyen in view of Nevis. As

indicated in the analysis above, Nevis does not teach "**obtaining one or more measurement values** from a **table storing hashed values** from a **previous measurement** of a POST BIOS **if one or more of said bits in said register indicate one or more segments** of said flash memory storing said POST BIOS **have not been updated**," To the contrary, Nevis teaches updating an entire "BIOS Image" **if the hashed values match**.

Claim 2

Dependent claim 2 recites a method for "transmitting said obtained measurement values to a **Trusted Platform Module**". As an initial matter, there is no discussion or mention in Nguyen of "a **Trusted Platform Module**". Thus, paragraphs [0035] [0036] [0038] and [0039] does not support the Examiner's conclusion that Nguyen discloses a method for "transmitting said obtained measurement values to a **Trusted Platform Module**".

For these reasons, the Applicants respectfully request the withdrawal of the rejections under 35 U.S.C. § 103(a). This entire application is now believed to be in condition for allowance and such action is respectfully requested. The Applicants request that the Examiner call the undersigned if clarification is needed on any matter within this Amendment, or if the Examiner believes a telephone interview would expedite the prosecution of the subject application to completion.

Applicants have made every effort to present claims, which distinguish over the prior art, and it is believed that all claims are in condition for allowance. However, Applicants invite the Examiner to call the undersigned if it is believed that a telephonic interview would expedite the prosecution of the application to an allowance. Accordingly, and in view of the foregoing remarks, Applicants hereby respectfully request reconsideration and prompt allowance of the pending claims.

Although Applicants believe that all claims are in condition for allowance, the Examiner is directed to the following statement found in M.P.E.P. § 706(II):

> When an application discloses patentable subject matter and it is apparent from the claims and the applicant's arguments that the claims are intended to be directed to such patentable subject matter, but the claims in their present form cannot be allowed because of defects in form or omission of a limitation, the examiner should not stop with a bare objection or rejection of the claims. The examiner's action should be constructive in nature and when possible should offer a definite suggestion for correction. (emphasis added)

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-3829, and please credit any excess fees to such deposit account.

Date: July 21, 2008

Respectfully submitted,

/Steven M. Greenberg/
Steven M. Greenberg
Reg. No.: 44,725
Adam C. Underwood
Reg. No.: 45,169
Tel: (561) 922-3845
Customer Number 50594